COT Security Alert – Deadline for Remediation of DNSChanger-Infected Hosts

---

In late 2011, the FBI released information concerning a criminal operation known as "Operation Ghost Click." A malware associated with this operation changes the default Domain Name System (DNS) server IP address on infected hosts to that of a rogue DNS server operated by criminals, all without the user's knowledge. This allows the criminals to control which sites the infected user visits on the Internet and can be used to connect unsuspecting users to fraudulent websites. The FBI seized 100 servers responsible for this attack, however due to the effect of an immediate shutdown, a court order was obtained to delay the shutdown date to **July 9, 2012**. The effect of shutting down these servers is that all infected computers will immediately be unable to connect to the Internet until the malware and DNS configuration are remediated. This means that on July 9, 2012, all infected computers will immediately disconnect from the Internet until the default DNS IP address on their system is changed and DNSChanger malware is removed.

Antivirus providers such as McAfee have provided updates since late 2011 which clean and remove the DNSChanger malware in many variants. It cannot be guaranteed that all variants of the malware have been addressed. It also cannot be guaranteed that the correct DNS IP address has been restored on any machine where the malware was present and then removed.

The FBI has issued an instruction sheet to aid users in determining whether they are infected and how to correct the default DNS IP address. State users should depend on their IT department's instructions for any DNS corrections on state-owned machines. Home users should refer to the FBI instruction sheet linked in this email and follow it for their personally-owned computers. In addition, Google will be alerting users who are defaulted to one of the rogue DNS server IP addresses as the user searches on the Google search engine. See attached article.

Computers that are kept current on antivirus signature (.DAT) files and updates, operating system updates and third-party software updates are far more secure than those that are not. Home users are advised to set up automatic updates where available as part of normal maintenance.

FBI link:
http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf

Google's alert to users:

http://googleonlinesecurity.blogspot.com/2012/05/notifying-users-affected-by-dnschanger.html

Notice: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/ciso/

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/ciso/